PCT/EP 99 / 05879 #5 RH

BUNDESREPUBLIK DEUTSCHLAND

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

EJV

Bescheinigung

EP 99/5879

Die SCM Microsystems GmbH in Pfaffenhofen/Deutschland hat eine Gebrauchsmusteranmeldung unter der Bezeichnung

"Sicherheitssystem"

am 11. August 1998 beim Deutschen Patent- und Markenamt eingereicht.

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Gebrauchsmusteranmeldung.

Die Anmeldung hat im Deutschen Patent- und Markenamt vorläufig die Symbole G 07 C und G 07 F der Internationalen Patentklassifikation erhalten.

München, den 14. September 1999
Deutsches Patent- und Markenamt
Der Präsident
Im Auftrag

Faust

Aktenzeichen: 298 14 427.1

A 9161
06.90
11/98

PRINZ & PARTNER GbR
PATENTANWÄLTE
EUROPEAN PATENT ATTORNEYS
EUROPEAN TRADEMARK ATTORNEYS

Manzingerweg 7
D-81241 München
Tel. +49 89 89 69 80

11. August 1998

SCM Microsystems GmbH
Luitpoldstraße 6
85276 Pfaffenhofen

Unser Zeichen: S 4388 DE
HD/Hc

Sicherheitssystem

Die Erfindung betrifft ein Sicherheitssystem für die Identitäts- und Berechtigungsprüfung in einer gesicherten Kommunikationsumgebung.

Die Identitäts- und Berechtigungsprüfung erfolgt in einer gesicherten Kommunikationsumgebung in der Regel anhand von persönlichen Kennzeichnungen in Kombination mit einer Speicher- oder Chipkarte. Beispielsweise muß an einem Bankautomat zuerst eine Bankkarte und dann eine persönliche Geheimzahl des Benutzers eingegeben werden. Wie die Erfahrung zeigt, sind derartige Identitäts- und Berechtigungskontrollen nicht ausreichend, um jeden Mißbrauch zu verhindern. Die Eingabe der persönlichen Geheimzahl ist nicht nur umständlich, sie kann auch relativ leicht ausspioniert werden.

Als sehr sicher gelten Identitäts- und Berechtigungsprüfungen mittels eines Fingerabdruck-Sensors. Es sind hoch auflösende, nach dem Prinzip einer kapazitiven Matrix arbeitende Sensoren bekannt, die von einem Fingerabdruck eine eindeutige und unverwechselbare Charakteristik ableiten und nach einer hochwirksamen Datenreduktion als Kenngröße zur Verfügung stellen. Diese Kenngröße kann in einer

Anwendung als Zugangs- und Berechtigungsbedingung abgespeichert werden. In einem solchen System ist die Eingabe eines persönlichen Geheimcodes überflüssig. Es ist aber prinzipiell nicht auszuschließen, daß die von dem Fingerabdruck-Sensor gelieferte Kenngröße auf ihrem Übertragungsweg abgefangen oder ausspioniert wird.

Durch die Erfindung wird ein Sicherheitssystem geschaffen, das bei Verzicht auf die Eingabe eines persönlichen Geheimcodes einen sehr hohen Schutz bietet. Gemäß der Erfindung enthält das Sicherheitssystem einen Chipkartenleser im Format einer PC-Karte, auf der personenbezogene Daten gespeichert sind. An den Chipkartenleser ist ein Fingerabdruck-Sensor angekoppelt. Eine Validierungseinrichtung validiert die von der Chipkarte gelesenen personenbezogenen Informationen in Abhängigkeit von Daten, die von dem Fingerabdruck-Sensor geliefert werden. Für den positiven Ausgang einer Identitäts- und Berechtigungsprüfung ist es notwendig, daß sowohl die Chipkarte mit den personenbezogenen Daten verfügbar ist als auch die von dem Finterabdruck-Sensor gelieferte Kenngröße den auf der Chipkarte gespeicherten personenbezogenen Daten korrekt zugeordnet ist.

Mit dem erfindungsgemäßen Sicherheitssystem läßt sich eine hochgradig gesicherte Kontrolle über die Kommunikation zwischen einem lokalen Datenverarbeitungsgerät und einem Netzwerk aufbauen. Gemäß einem ersten Lösungsansatz, bei dem der Fingerabdruck-Sensor in den Chipkartenleser integriert ist, enthält das Sicherheitssystem eine Schnittstelle für den Anschluß an das Netzwerk. Bei dieser Schnittstelle kann es sich um einen üblichen Netzwerkadapter, ein Modem oder eine IR-Schnittstelle handeln. Die Kommunikation zwischen dem lokalen Datenverarbeitungsgerät und dem Netzwerk kann nur über das Sicherheitssystem erfolgen. Durch ein solches Sicherheitssystem kann gewährleistet werden, daß nur berechtigte Benutzer auf das Netzwerk zugreifen können. Ferner kann vorgesehen sein, daß alle in einer oder in beiden Richtungen übertragenen Nachrichten durch die von dem Fingerabdruck-Sensor gelieferte Kenngröße signiert und somit authentifiziert werden.

Ein zweiter Lösungsansatz besteht darin, den Fingerabdruck-Sensor an einem mit dem Chipkartenleser durch eine lösbare Steckverbindung

gekoppelten Modul anzuordnen. Um bei dieser Lösung ein Ausspionieren der von dem Fingerabdruck-Sensor gelieferten Kenngröße im Bereich der Steckverbindung zu verhindern, wird diese Kenngröße nicht unmittelbar, sondern verschlüsselt übertragen. Zu diesem Zweck verfügt das Modul über einen SAM-Kartenleser und einen internen Prozessor. Auch mit einer solchen Ausführung des Sicherheitssystems läßt sich die Kommunikation zwischen einer lokalen Datenverarbeitungseinrichtung und einem Netzwerk oder dergleichen mit einem Höchstmaß von Sicherheit kontrollieren.

Weitere Merkmale und Vorteile der Erfindung ergeben sich aus der folgenden Beschreibung und aus der Zeichnung, auf die Bezug genommen wird. In der Zeichnung zeigen:

Figur 1 eine schematische Seitenansicht eines Chipkartenlesers mit eingeschobener Chipkarte und angestecktem Sensormodul;

Figur 2 eine Stirnansicht des Sensormoduls;

Figur 3 eine Draufsicht des Sensormoduls mit abgeschnitten dargestellter Chipkarte;

Figur 4 drei mögliche Ausführungsformen für das Gehäuse des Sensormoduls;

Figur 5 eine schematische Seitenansicht des Chipkartenlesers und des Sensormoduls gemäß einer weiteren Ausführungsform;

Figur 6 eine Stirnansicht des Sensormoduls;

Figur 7 eine Draufsicht des Sensormoduls;

Figur 8 eine schematische Seitenansicht einer weiteren Ausführungsform des Chipkartenlesers mit Sensormodul; und

Figur 9 ein Blockschaltbild des Sicherheitssystems.

Das in Figur 1 gezeigte Sicherheitssystem für die Identitäts- und

Berechtigungsprüfung in einer gesicherten Kommunikationsumgebung enthält einen Chipkartenleser 10 im Format einer PC-Karte und einen Sensormodul 12, der einen Fingerabdruck-Sensor 14 aufweist und durch eine Steckverbindung lösbar mit dem Chipkartenleser 10 gekoppelt ist. Der Chipkartenleser 10 weist einen Aufnahmekanal für eine Chipkarte 16 und ein in dem Aufnahmekanal angeordnetes Kontaktfeld 18 zur Kontaktierung der Chipkarte 16 auf. Bei der hier gezeigten Ausführungsform ist der Aufnahmekanal für die Chipkarte zwischen einer Deckelplatte 10a und dem Hauptkörper 10b des Chipkartenlesers gebildet.

Das Sensormodul 12 ist an die schmale Stirnfläche des Chipkartenlesers 10 angekoppelt, aus der die Chipkarte 16 herausragt. Für den Durchgang der Chipkarte 16 ist das Gehäuse des Sensormoduls 12 mit einem Schlitz 20 versehen. In die obere Hauptfläche des Sensormoduls 12 ist der Fingerabdruck-Sensor 14 eingelassen. Zwei Führungsstifte 24 des Sensormoduls 12 sind in entsprechende Aufnahmeöffnungen an der schmalen Stirnseite des Chipkartenlesers 10 einführbar. Eine Reihe von Kontaktstiften 26 des Sensormoduls 12 ist in entsprechende Kontaktöffnungen an derselben Stirnseite des Chipkartenlesers 10 einführbar. An den Schmalseiten des Sensormoduls 12 sind Betätigungselemente 28 für eine Verriegelungseinrichtung angebracht, mittels welcher das Sensormodul 12 lösbar mit dem Chipkartenleser 10 verrastet wird. In Figur 3 ist auch die Kontaktfläche 16a der Chipkarte 16 eingezeichnet. Sie kommt bei in den Chipkartenleser 10 eingeschobener Chipkarte 16 unter dem Kontaktfeld 18 zu liegen.

Je nach Anordnung des Aufnahmekanals für die Chipkarte 16 im Chipkartenleser ist am Gehäuse des Sensormoduls 12 der in Figur 2 zu erkennende Schlitz 20 oder aber eine Aussparung 20a an der Unterseite bzw. eine Aussparung 20b an der Oberseite des Sensormoduls 12 angebracht, wie in Figur 4 veranschaulicht.

Bei der in Figur 5 gezeigten Ausführungsform ist an dem Sensormodul 12 ein Gehäuseblock mit einer rampenförmigen Auflagefläche gebildet, in die der Fingerabdruck-Sensor 14 eingelassen ist. Ferner ist das Sensormodul 12 zur Aufnahme und zum Auslesen einer sogenannten SAM-Karte oder SIM-Karte 32 ausgebildet. Bei dieser Karte handelt es sich um einen bekannten Sicherheits- und Authentifizierungs-Modul.

Bestandteil des Sensormoduls 12 ist ferner eine Schnittstelle für den Anschluß an ein Kommunikationssystem; bei der gezeigten Ausführungsform ist dies ein Netzwerk-Adapter, an den ein Netzwerkkabel 34 mittels eines Steckverbinders 36 angeschlossen wird.

Figur 8 zeigt eine Ausführungsform des Chipkartenlesers mit einem Aufnahmekanal für die Chipkarte, der zwischen einer Bodenplatte und dem Hauptkörper des Chipkartenlesers gebildet ist.

Anhand des Blockschaltbilds in Figur 9 wird nun das dem Sicherheitssystem zugrunde liegende Konzept erläutert.

Das aus dem Chipkartenleser 10 mit Chipkarte 16 einerseits und dem Sensormodul 12 mit Fingerabdruck-Sensor 14 und SAM-Karte 32 andererseits bestehende Sicherheitssystem ist zwischen ein als Host bezeichnetes Datenverarbeitungsgerät (PC) und einen Netzwerkanschluß eingefügt. Der Chipkartenleser 10 verfügt ebenso wie das Sensormodul 12 über einen eigenen lokalen Bus. Über die Steckverbindung zwischen Chipkartenleser 10 und Sensormodul 12 sind die beiden Bussysteme miteinander gekoppelt. Der Chipkartenleser 10 enthält einen internen Prozessor 40, der die Funktionen Authentifizierung, Identifizierung, kryptographische Verschlüsselung und Signatur übernimmt. Auf der Seite des Host ist der Chipkartenleser 10 mit einer geeigneten Schnittstelle 42, insbesondere einer PCMCIA-Schnittstelle ausgestattet. Ferner beinhaltet der Chipkartenleser 10 einen Speicher 44 für gesicherte Daten in Flash-Technologie und eine Zeitstempel-Einheit 46, die einen Funkuhr-Modul beinhalten kann. Die Chipkarte 16 ist als sogenannte Smartcard ausgebildet und enthält eigene Prozessor- und Speicherschaltungen. In der Chipkarte 16 sind insbesondere persönliche Schlüssel und Codewörter zum Zweck der Identitäts- und Berechtigungsprüfung abgelegt. Alle genannten Bestandteile des Chipkartenlesers 10 sind an dessen internen lokalen Bus angekoppelt.

Das Sensormodul 12 enthält ebenfalls einen internen Prozessor 50, dessen Aufgabe insbesondere die Analyse der von dem Sensor 14 gelieferten Fingerabdruck-Daten zum Zweck der Identifizierung ist. Die SAM-Karte wird über eine Kontakteinheit 52 ausgelesen. Auf der SAM-Karte

sind Fingerabdruck-Kenndaten des berechtigten Benutzers gespeichert. Die Kommunikations-Schnittstelle des Sensormoduls 12 umfaßt eine Schnittstellen-Steuereinheit 54 und einen Netzwerkadapter 56, an den das Netzwerkkabel 34 angeschlossen wird.

Die SAM-Karte enthält zusätzlich zu den Fingerabdruck-Kenndaten des berechtigten Benutzers Daten und Strukturen zur Verschlüsselung dieser Daten, die dann in verschlüsselter Form an den Chipkartenleser 10 zur Auswertung übergeben werden.

Auf eine verschlüsselte Übertragung der Fingerabdruck-Daten kann verzichtet werden, wenn Fingerabdruck-Sensor und Chipkartenleser miteinander integriert sind, so daß ein Abfangen der Daten vom Fingerabdruck-Sensor nicht möglich ist. Bei dieser alternativen Ausführungsform wird auch die Kommunikationsschnittstelle (Netzwerkadapter) in dem System integriert.

PRINZ & PARTNER GbR

PATENTANWÄLTE
EUROPEAN PATENT ATTORNEYS
EUROPEAN TRADEMARK ATTORNEYS

Manzingerweg 7
D-81241 München
Tel. +49 89 89 69 80

11. August 1998

SCM Microsystems GmbH
Luitpoldstraße 6
85276 Pfaffenhofen

Unser Zeichen: S 4388 DE
HD

Schutzansprüche

1. Sicherheitssystem für die Idenitäts- und Berechtigungsprüfung in einer gesicherten Kommunikationsumgebung, mit

- einem Chipkartenleser im Format einer PC-Karte; - einer Chipkarte, auf der personenbezogene Daten gespeichert sind;
- einem Fingerabdruck-Sensor, der mit dem Chipkartenleser gekoppelt ist;
- einer Validierungseinrichtung zu Validierung der von der Chipkarte gelesenen personenbezogenen Informationen in Abhängigkeit von Daten, die von dem Fingerabdruck-Sensor geliefert werden.

2. Sicherheitssystem nach Anspruch 1, dadurch gekennzeichnet, daß der Fingerabdruck-Sensor an einem mit dem Chipkartenleser durch eine lösbare Steckverbindung gekoppelten Modul angeordnet ist.

3. Sicherheitssystem nach Anspruch 2, dadurch gekennzeichnet, daß das Modul auf eine schmale Stirnfläche des Chipkartenlesers, an der die Chipkarte herausragt, aufsteckbar ist.

5. Sicherheitssystem nach Anspruch 3, dadurch gekennzeichnet, daß in dem Modul ein Schlitz für den Durchgang der Chipkarte angeordnet ist.

6. Sicherheitssystem nach einem der Ansprüche 2 bis 5, dadurch gekennzeichnet, daß das Modul einen SAM- oder SIM-Kartenleser beinhaltet.

7. Sicherheitssystem nach Anspruch 6, dadurch gekennzeichnet, daß die von dem Fingerabdruck-Sensor gelieferten Daten mit den von der SAM-bzw. SIM-Karte gelesenen Daten in einem internen Prozessor des Moduls zu einer verschlüsselten Identitätsinformation verarbeitet werden.

8. Sicherheitssystem nach einem der Ansprüche 1 bis 7, gekennzeichnet durch eine Schnittstelle für den Anschluß an ein Kommunikationssystem, insbesondere Netzwerk.

9. Sicherheitssystem nach den Ansprüchen 2 und 8, dadurch gekennzeichnet, daß die Schnittstelle in dem Modul enthalten ist.

10. Sicherheitssystem nach Anspruch 8 oder 9, dadurch gekennzeichnet, daß über die Schnittstelle signierte Nachrichten mit der Kommunikationsumgebung austauschbar sind.

Gebrauchsmusteranmeldung vom 11. August 1998
SCM Microsystems GmbH
Sicherheitssystem

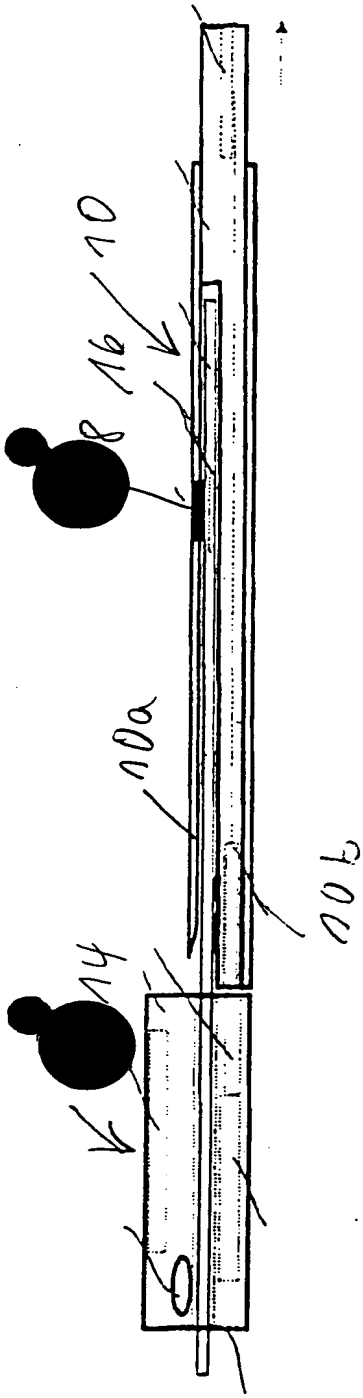


Fig. 1

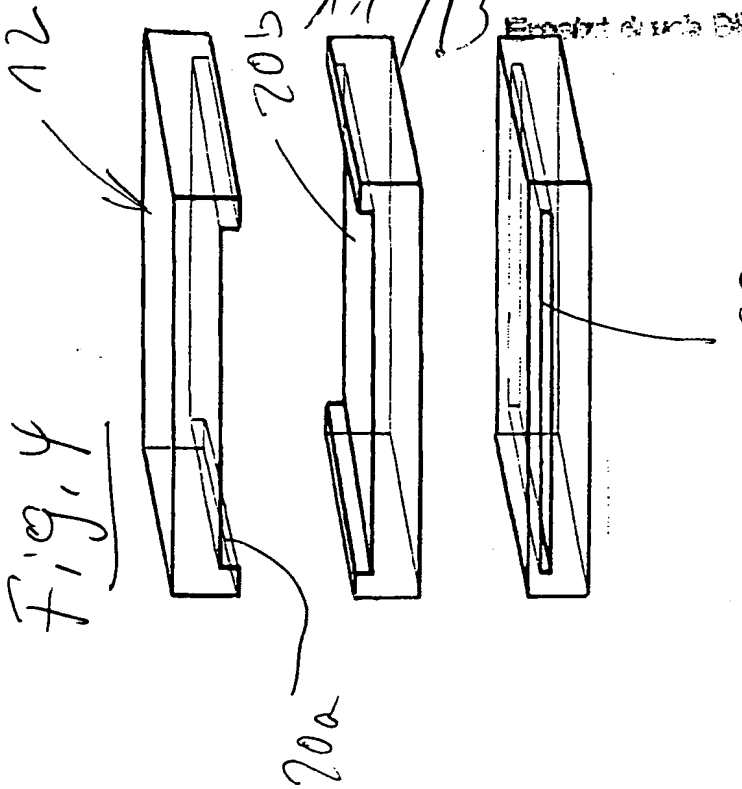


Fig. 4

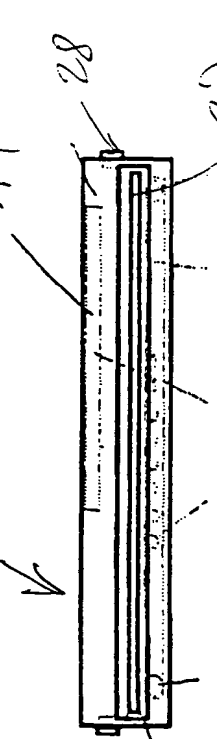
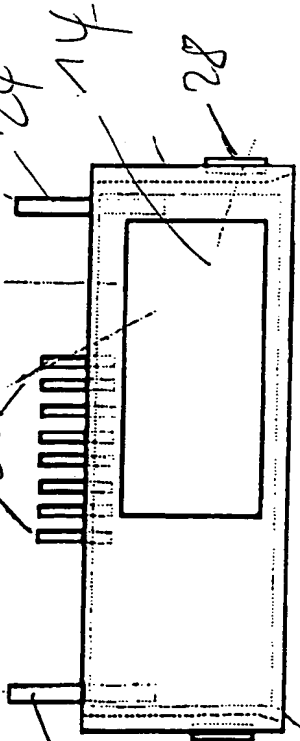


Fig. 2



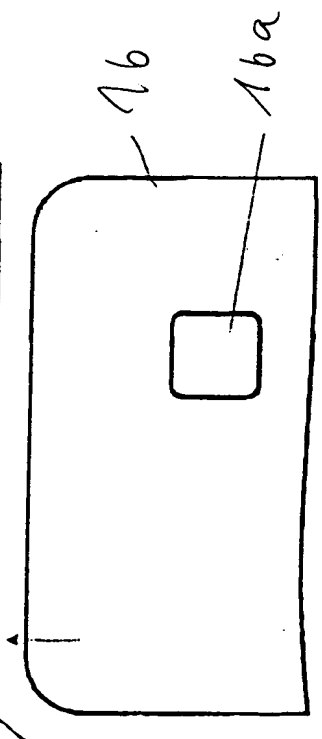
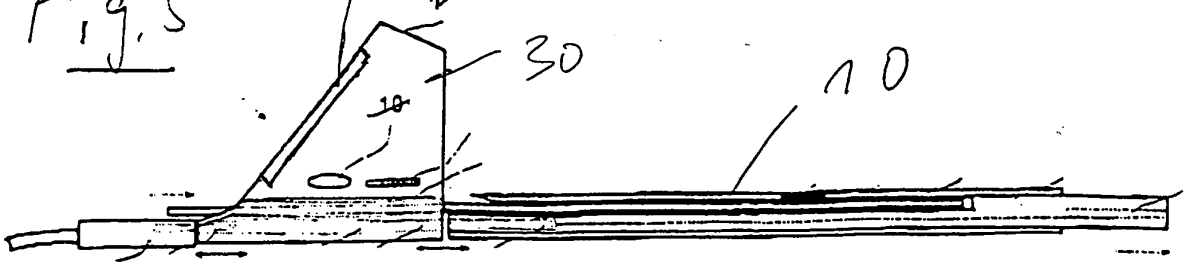


Fig. 3

Fig.5



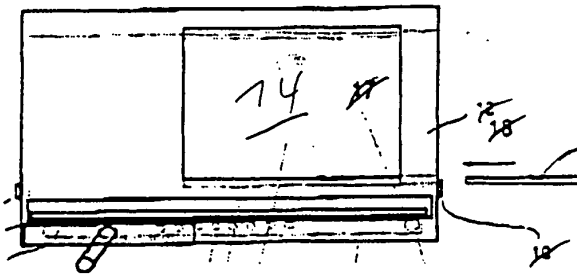


Fig.6

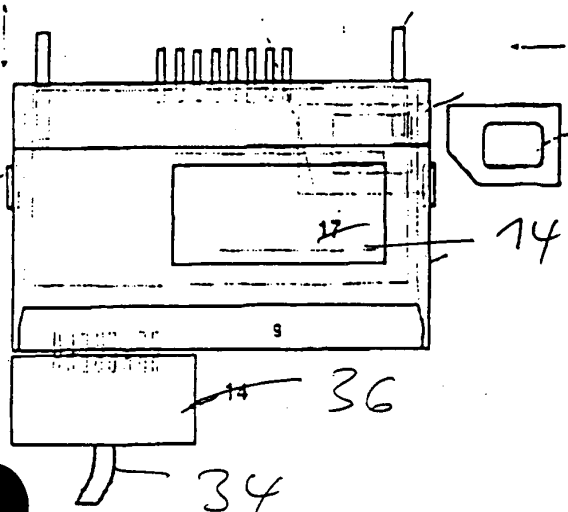
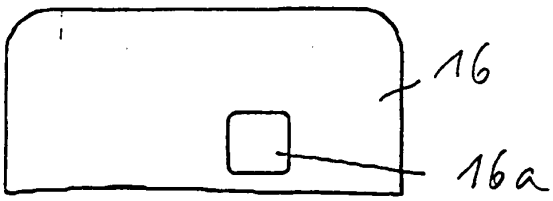


Fig.7



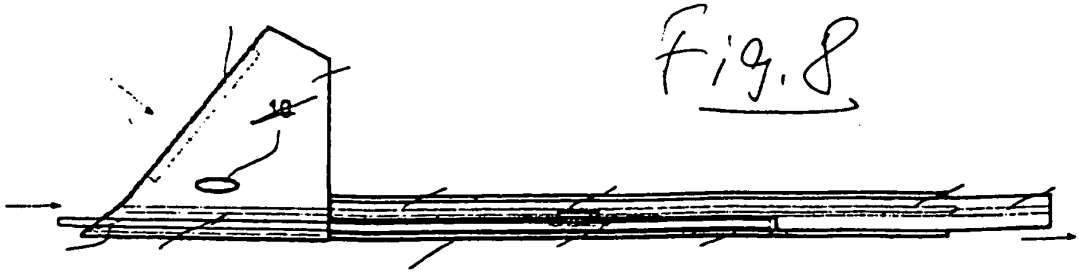


Fig.8

Gebrauchsmusteranmeldung vom 11. August 1998
SCM Microsystems GmbH
Sicherheitssystem

Fig. 9